4-1-2012

Access Control Hygiene and the Empathy Gap in Medical IT

Yifei Wang
Dartmouth College

Sean Smith
Dartmouth College

Andrew Gettinger
Dartmouth College

Access Control Hygiene and the Empathy Gap in Medical IT

Yifei Wang
yifeiwang2012@gmail.com

Sean Smith
sws@cs.dartmouth.edu

Andrew Gettinger
andrew.gettinger@dartmouth.edu

Dartmouth College
Computer Science Technical Report TR2102-713
April 2012

Abstract

In theory, access control is a solved problem. In practice, large real-world enterprises still report trouble: de facto policy becomes unmanageable; users circumvent controls. These issues can be particularly critical in medical IT, such as emerging EMR and EHR, where access control errors can have serious repercussions. In this paper, we investigate how real-world EMR users think about access control when they are making policy decisions in the abstract–and when they are actually using the system in treatment scenarios. Mismatches suggest places ("empathy gaps") where new policy tools may be needed.

1 Introduction

The *Electronic Medical Record (EMR)* is an effort aimed at the comprehensive digital integration of medical information formerly spread across a variety of traditional paper-based systems held by an enterprise in the healthcare industry; the related *Electronic Health Records (EHR)* reaches across enterprises [5]. More and more industries are replacing their old fashioned systems with an integrated computerized system to manage business data, perform business operations and offer services to customers. Healthcare is no exception.

An integrated electronic integrated system would clearly offer advantages to both the care providers and the patients receiving the services: for example, in cost savings, efficiency, automatic alerts and reminders, and reduced error from illegible handwriting (e.g.,[7]).

However, the shift to EMR and EHR does pose many problems. For now, let's consider the smaller challenge of EMR. As should come as no surprise to the reader, an area of particular concern for an EMR is the huge challenge to satisfy its users regarding privacy, confidentiality, and security. Providing medical records with high availability, yet maintaining their protection from unauthorized access is a complex yet crucial task. Problems here risk endangering the health condition and even risking lives of the patients (not to mention exposing the enterprise and clinicians to regulatory and legal punishments).

Access Control Hygiene In computer security, *access control* addresses the problem of who can do what in an information system. In the initial view, we imagine an access control *policy* as a matrix consisting of the *subjects* (actors) versus the *objects* (resources); the entries in a particular subject-object cell specify the current things that subject is allowed to do with that object. Research and practice has given rise to more elaborate models and tools, such as *role-based access control* (e.g, [12]) and *experience-based access management* (e.g., [6]). (Some researchers even formalize notions of *optimistic* security: assuming that subjects are allowed access, and trying to discover and straighten out problems afterwards [9].)

In theory, an enterprise sets the right access control policy that permits all the necessary access and blocks all the bad ones, and installs the right IT to monitor and enforce this policy. Unfortunately, it is often reported that in large enterprises, the policy followed in practice quickly devolves into an unmanageable spaghetti of shared passwords, post-it notes, and other circumvention. One researcher termed this the *access control hygiene* problem [2].

As literature reports (e.g., [8]) and as we have seen in our own fieldwork (e.g., [13, 14]), healthcare is no exception. Indeed, the overwhelming urgency to take care of the sick can lead to an environment where availability of information dominates all other security concerns. (We even had one clinician ask if we wanted to "help patients" or merely "build a better policeman.") We have even seen medical enterprises dispense with access control policy altogether, defaulting to "always allow" and hoping audit catches abusers.

Crafting access control policy for computer-mediated data systems such as EMRs has always been a crucial task and a difficult problem. An overly "loose" policy might permit inappropriate access, but an overly "tight" policy might prevent appropriate access and encourage user circumvention, which may lead to equally serious consequences. The policies are especially crucial since the healthcare field poses a number of difficulties and challenges not faced in other security environments. For a start, the information being protected is highly personal and maybe even lethal—security breeches may lead to irrevocable consequences for the individuals involved and might put the individuals physical health or even life at serious risk. Yet, at the same time, there is a need in emergencies to access all the information relevant to the conditions of a patient in order to provide a more accurate evaluation of a patient's health condition and provider better treatment.

This situation lead to two fundamental problems.

- First, why does it seem so hard, in practice, to create the right access control policy for large enterprise EMRs?
- More subtly, how can we measure the amount of circumvention that takes place in real-world EMR? Each such act risks punishment for the actor and the enterprise, making direct study infeasible; however, science needs data, not just anecdotes.

In this paper, we explore a novel direction to try to shed light on these problems. Section 2 reviews related work. Section 3 presents the approach we take. Section 4 presents our experimental methods. Section 5 presents our overall results, and Section 6 presents some analysis for demographic subgroups. Section 7 discusses implications for EMR access control security, and Section 8 concludes.

2 Related Work

As mentioned earlier, Koppel et al [8] cataloged a large number of ways clinicians worked around a computer-based prescription system, in ordered to get their jobs done.

The emergence of computerized medical records gives rise to physician workarounds, which not only defeats the purpose of a computerized system of medical records but also introduces a negative impact on work practices. In their study [11], Saleem et al found that clinicians created their own tools and shadow processes to support their work when they believed that the computer system caused them inconvenience. The most common practice was for the doctors and nurses to write down their findings on a piece of paper and transfer to other physicians, which carried the risk that medical orders would not be entered into the electronic health record, potentially creating gaps in documentation or even unintended leaks of critical patients' medical information. Another common workaround was the creation of electronic spreadsheets, on a local or personal machine, because the medical professionals found this to be a more convenient and flexible way to deal with their data.

Ferreira et al reviewed [4] a decade of published literature on access control policies in the healthcare industry. Of almost three dozen papers, these authors only four systems where end users (as opposed to enterprises or larger entities) could set policy—but none of these were in fact implemented. Furthermore, in none of the described systems described policies whose creators included end-users. The authors conclude this lack of involvement of the EMR end-users is a fundamental obstacle to effective use.

A better understanding of how the access control systems are designed and implemented can thus lend insights on why such practices occur and how the barriers can be overcome to produce a successful integration of EMR system in the healthcare industry. As Ferreira et al note, such an understanding might best start with the users.

Moving away from policy technology itself, in earlier work [15] in our own lab, we examined how end users in social networks interacted with policy technology—and showed how an earlier psychological result that "introspection inhibits intuition" applies. Making such users think about setting policies leads to counter-intuitively open policies.

3 Our Approach

To approach the access control hygiene problem in medical IT, we thus decided to look at how real medical users think about access control decisions in EMRs. Anecdotally, the medical community creates policies that medical users seem to often find too constraining, requiring workarounds.

Suppose we eliminate the gap that worried Ferreira and assume the end-user population is also the population setting the policy. Is there something different about how humans make judgments in these two different settings?

The psychology literature offers experimental results regarding this *empathy gap* (e.g., [3]). Humans can indeed make quantitatively different decisions when they are directly embedded in a situation versus when they are reasoning about it abstractly (e.g, [1]); even making decisions for one's self in the future can be like reasoning about others in the abstract (e.g., [10]).

We thus prepared an experiment to see if this empathy gap plays a role in the access control hygiene problem. In collaboration with medical colleagues, we developed a corpus of EMR access control questions, each consisting of a scenario and a decision to be made. For each question, we prepared two versions:

- a *control* version, phrased in an abstract, role-based way (per the teachings of HIPAA on EMR access control best practices), and
- an *experimental* version, putting the subject in a hypothetical instantiation of that scenario.

(See the Appendix.)

We recruited real-world EMR users, divided them into a control group and experimental group, and gave each group the corresponding questions. If we find significantly different answers, that would suggest that reasonable real-world EMR users might make policies that reasonable real-world EMR users might be motivated to subvert—hence identifying trouble spots for access control hygiene.

4 Methods

The subjects who participated in this study consisted of 164 participants—78 in the experimental treatment group and 86 in the control group. As noted above, the experimental group received a treatment effect that induces subjective experience on the user comparing to the control group. The subjects were composed of staff members a partner tertiary care research and teaching hospital. The subjects included clinicians at different stages of their professions (doctors, nurses, residents, and medical students), as well as non-clinicians (IT staff, administrators, billing specialists, etc.).

Subjects were recruited by an email from the medical informatics group asking for volunteers to participate in a study that examines perspectives relative to access to and the privacy of medical records electronically. Subjects first responded to the email to show interest in participating in the 15-minute study. The names of interested participants were then collected and randomly assigned into either the subjective experiment group or the control group—we would thus expect that demographic attributes of the participants in the two groups will be roughly equivalent and therefore any effect observed between two groups can be linked to the treatment effect—and is not likely a result of the different characteristic of the individuals in the group. Another email with the link to the survey was then sent out to each participant. This study was approved by the Committee for the Protection of Human Subjects, the Institutional Review Board at Dartmouth College.

Surveys taken by both groups were composed on `surveymonkey.com` and the participants were given links to those surveys. We designed a simulated healthcare record system that deals with patient information access and control issues that are common in daily hospital settings and which may touch on information access de facto best practices not necessarily incorporated in current systems. Members of each group completed a questionnaire that presented them with scenarios in our simulated EHR and asked them to make access control decisions for the new system. (Subjects were instructed that the scenarios were hypothetical; in particular, this was not a test of how well they followed enterprise rules.)

The subjects were asked whether a certain action should or should not be allowed under a particular circumstance. As noted above, we designed the experiment so that the two groups were given the

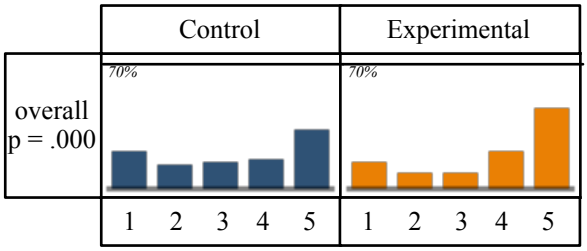

Figure 1: Overall, the populations differed significantly. (The graphs show histograms of Likert answers.)

same situation and the same actions except that in the group with the treatment effect, we introduced a more subjective experience of the scenario in question on the person who is making access control decisions.

We phrased the questions so as to collect answers on a Likert scale, from 1 to 5, with 1 corresponding to a more restrictive policy and 5 to a more open one.

For analysis, we thus ended up with pairs of sample sets of Likert ratings. We used an F test to determine whether the variances were equal; on the basis of that, we used a t-test to see if the data warranted ruling out the null hypothesis that any difference in the samples was due to random noise.

5 Results

Figure 1 through Figure 3 show our overall results.

A priori, one might have predicted that the experimental group (testing what it's like to use an EMR) would be make more permissive decisions than the control group (testing what it's like to create a policy), but wonder whether the difference would be statistically significant ($p < 0.05$). Figure 1 shows that overall, both outcomes held.

However, looking at the data by individual question reveals some surprises. (To simplify presentation in this report, we sorted the questions by decreasing significance of difference.) First, the populations differed significantly in only nine of the thirteen questions (Figure 2). In four of the thirteen, there was no difference (Figure 3) Why? Why don't these scenarios reveal the empathy gap?

Furthermore, among the nine questions where the subjects appeared to exhibit an empathy gap, the

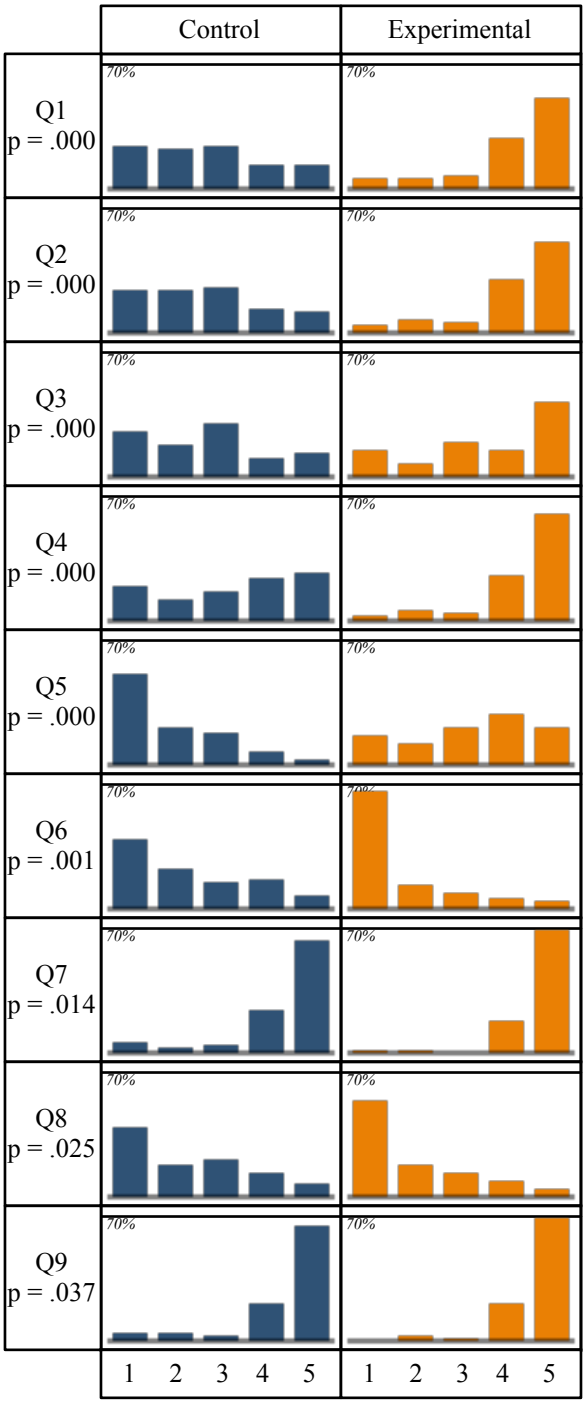

Figure 2: On nine questions, the populations differed significantly. Note, however, that on Q6 and Q8, the experimental group became *more* conservative! (The graphs show histograms of Likert answers.)

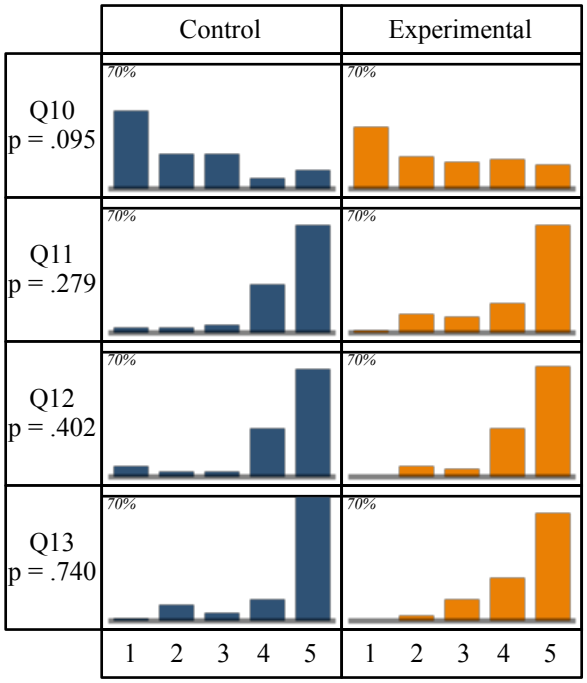

Figure 3: On four questions, the populations did not differ significantly. (The graphs show histograms of Likert answers.)

experimental group made looser access control decisions (that is, indicating they might feel justified in circumventing controls) in only seven. In the other two scenarios (Q6 and Q8), the experimental group made *tighter* access control decisions. What's going on here? (It's as if frustrated end-users want to circumvent the system in order to *add* more controls!)

6 Demographic Groups

Our partner medical enterprise provided us a large set of test subjects distributed throughout the staff. As part of the survey, we gathered basic demographic information, allowing us to partition the subjects into various demographic groups among this population. As a consequence, we decided to also look at differences in access control judgments based on these demographics.

We partitioned the populations four different ways:

- by years of service (less than 10, 10-20, or over 20);
- by role at the hospital (physician, nurse, or admin/tech);
- by age (less than 40, 40-50, or over 50); and
- by gender (male, female).

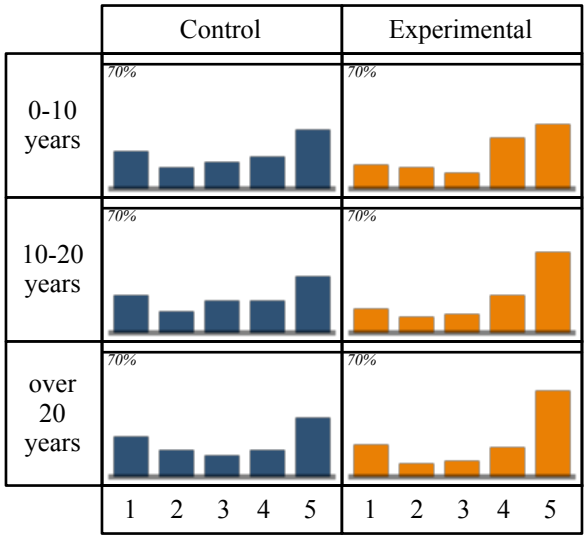

Figure 4: Histograms of answers when we partition subjects by years of experience.

For each partition, we examined how each subgroup compared to its overall group—e.g., "nurses in the control group" versus "everyone in the control group"—over all the questions. We also compared how each subgroup compared to its corresponding subgroup in the other test—e.g., "nurse in the control group" versus "nurses in the experimental group". However, this latter set of comparisons showed every pair with statistically significant differences—which is not very interesting.

For this paper, we did not yet do a finer-grained analysis looking at subsets of the questions.

Figure 4 shows the results when we partition by years of service. Although we saw no statistically significant differences, we do see a slight skewing to the extremes when we move to the most experienced users. Whether setting policy or complaining about it, they seem to be more sure of themselves.

Figure 5 shows the results when we partition by role in the hospital. Here, we see that, in the control group, the admin/tech staff made significantly different decisions from whoever wasn't in that role—visually, we can see the distribution is flatter. (Perhaps the medical training the other roles receive

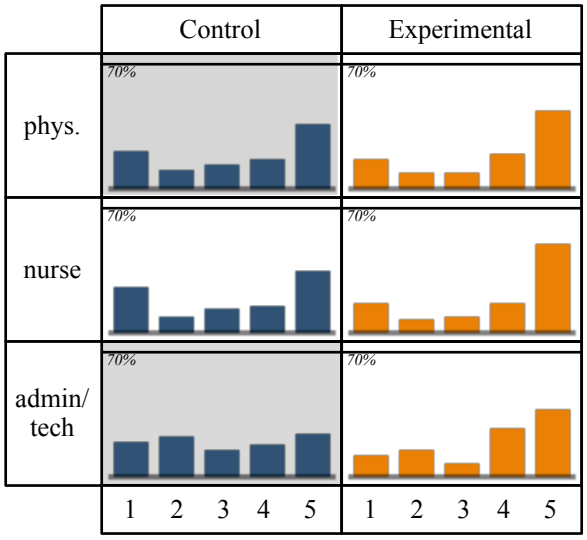

Figure 5: Histograms of answers when we partition subjects by roles. The grayed-out boxes indicate interesting differences: within the control group, admin/tech subjects differed significantly from non-admin/tech ($p = 0.018$)); physicians also differed from non-physicians ($p = 0.049$).

makes them more confident?) Similarly, the control physicians differed from non-physicians, but with a more non-flat distribution—supporting the training/confidence link.

Interestingly, these differences vanish when the subjects are asked to make the same decisions subjectively.

Figure 6 shows the results when we partition by age. Here, we see that the middle-aged experimental group makes significantly different decisions—-they seem more sure of themselves, and more permissive, then the experimental groups at other ages. The younger experimental group differs significantly the other way: they seem less sure of themselves.

Interestingly, these differences did not show up when we asked subjects to make the same decisions, but in a more abstract way.

Figure 7 shows the results when we partition by gender. Here, we see that, within each group. the genders make significantly different decisions. In both cases males seem less sure of themselves than females. However, males also have more "5" answers, suggesting they are more permissive; it is interesting to note that Trudeau et al [15] found something similar in social networks.

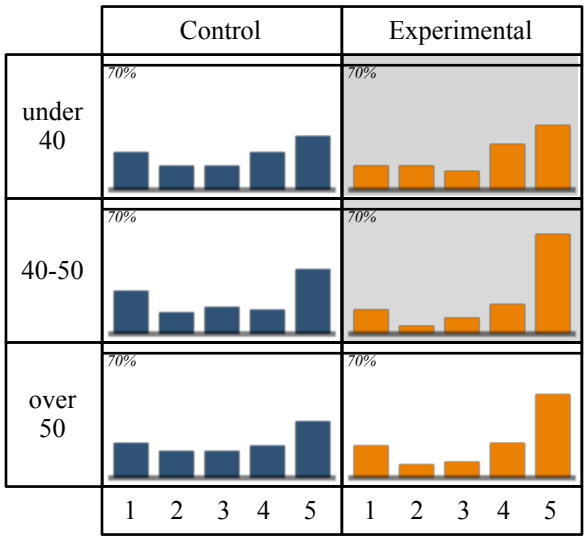

Figure 6: Histograms of answers when we partition subjects by age. The grayed-out boxes indicate interesting differences: within the experimental group, under-40 differed from the rest ($p = 0.025$); 40-50 also differed from the rest ($p = 0.012$).

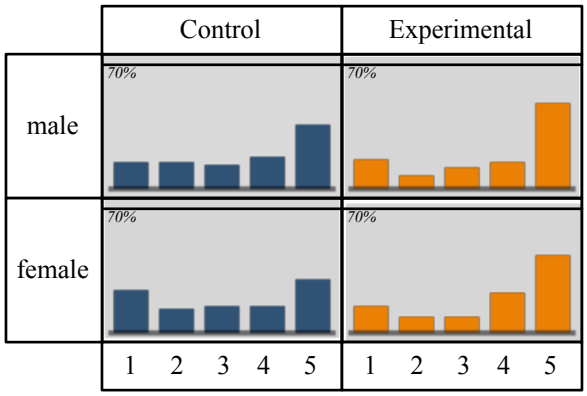

Figure 7: Histograms of answers when we partition subjects by gender. In both the control and experimental groups, the genders differed from each other significantly ($p = 0.001$).

7 Implications

In seven of the thirteen scenarios, reasonable EMR users would make access control policy decisions that reasonable EMR users would find overly constraining. What this implies for EMR access control depends on what stakeholders feel is the "correct" access control decision in these scenarios. If the more conservative decision is desirable, then health enterprises might wish to apply more education and stronger controls and auditing in these settings, since the results suggest that end-users will be frustrated here, and may be tempted to circumvent the system. If stakeholders are ambivalent about the "correct" decision, then health enterprises may wish to switch towards a "break-glass"/auditing model in these settings; frustrated end users can then take the actions they feel necessary—but will need to justify their actions later.

On the hand, if stakeholders feel that the control group decisions were systematically too restrictive in these scenarios, then the results suggest that perhaps researchers need to explore different ways of setting policies. Rather than thinking in abstract terms ("should a physician in setting X be allowed to Y?"), thinking in terms of specific subjective experiences ("should *I* be allowed to do this *right now*?") would enable policy-makers to make more accurate policies. (Perhaps we need to begin experimenting with alternative policy-creation tools—"audit to allow" for humans.)

Although it's tempting to suggest "involve more end-users in policy creation," we note that this result may imply this suggestion is not sufficient—in our test, the policy makers *were* end-users, so something more is needed.

In four of the thirteen scenarios, reasonable EMR users would make access control policy decisions that reasonable EMR users would find just fine in practice. If an enterprise is currently shying away from enforcing access control, for fear of pushback by frustrated users, these results imply that deploying tighter controls in these settings will be acceptable.

In two of the thirteen scenarios, reasonable EMR users would make access control policy decisions that were *looser* than what reasonable users would want in practice. The implications here require further thought.

The above discussion suggests an overarching challenge: what is it that led to the usage scenarios falling into these different classes? What procedure can stakeholders use in general to tell which class a given new scenario falls into? Although further analysis is required here, we offer some tentative observations:

- In the backwards cases (Q6 and Q8), where the experimental group made tighter decisions, both involved non-medical staff getting access.

  Perhaps the work of the subjects in these two scenarios are perceived as less relevant to patient care.

- Two of the no-difference cases (Q11 and Q12) involved a clinician of "lower" status than a physician getting access; the others involved a physician, but with some extra separation from direct internal clinical care.

8 Conclusions

In this paper, we developed (with real-world medical practitioners) a set of representative EMR usage scenarios involving access control decisions. For each scenario, we produced two versions: an abstract version (such as one might encounter in crafting an RBAC policy) and a specific, subjective version (such as one might encounter in real treatment settings). We then recruited a large set of real-world EMR users from a partner hospital, partitioned them into two groups, and gave each group one version of the scenarios. The resulting analysis showed that in many cases, the subjective group made significantly looser decisions. In these settings, it would appear that effective a priori policy construction is hampered by an "empathy gap." Identifying these scenarios and reducing the gap might help improve usability and security of medical IT.

Acknowledgments

This work is supported in part by the US National Science Foundations Trustworthy Computing award #0910842 and by Google; however, views and conclusions are the authors' alone.

We are especially grateful to our colleagues in this project—and to the anonymous medical institution who permitted their staff to be subjects in this experiment.

Appendix: Access Control Scenarios

In our control group, we asked standard, non-subjective access control questions, as if the subject was making an RBAC policy decision for the EMR. In the experimental group, we asked about the exact same scenarios, only in a personal and subjective way—as if the subject using the EMR.

To aid in clarity of presentation, we enumerated the questions in this report by significance of difference. In this Appendix, we further subdivide into the three groups of interest

In this first group of questions, the subject decisions differed significantly ($p < 0.05$), with the experimental group making looser decisions:

C1: It is appropriate that the hospital privacy policy gives local addiction treatment programs full access to a patient's medical record if the patient is diagnosed with serious alcohol abuse.
E1: Patient Condition: Erica Brown is a patient diagnosed with serious alcohol abuse and was sent to the local addiction treatment program. Your Position/Relationship with the Patient: You are a physician who works at the local addiction treatment program. Erica was sent to you from the hospital. You would like to provide some treatment for Erica. Statement: It is appropriate that you gain access to all paper and electronic records of Erica's full medical history at the hospital.

C2: It is appropriate that the hospital privacy policy gives local addiction treatment programs full access to a patient's medical record if the patient is diagnosed with serious drug abuse.
E2: Patient Condition: Thomas Wagner is a patient diagnosed with drug abuse and was sent to the local addiction treatment program. Your Position/Relationship with the Patient: You are a physician who works at the local addiction treatment program. Thomas was sent to you and you would like to provide some treatment for Thomas. Statement: It is appropriate that you gain access to all paper and electronic records of Thomas' full medical history at the hospital.

C3: It is appropriate that the hospital privacy policy gives an attorney full access to a patient's medical record if he needs the patients information to perform essential legal operations.
E3: Patient Condition: Melissa Kenning is a patient who recently came to the hospital for consistent hypertension and is now suing the hospital for negligence. Your Position/Relationship with the Patient: You are an attorney who specializes in legal issues in medical practice. You have worked five years as a member of the legal staff at the hospital. You are assigned by the hospital to work on the lawsuit with Melissa. Statement: It is appropriate that you are able to see all paper and electronic records of Melissa's full medical history.

C4: It is appropriate that the hospital privacy policy gives local psychiatric hospitals or community mental health services full access to a patient's medical record if the patient is diagnosed with mental health problems.
E4: Patient Condition: Jake White is a patient diagnosed with serious mental health problems and was sent to the local psychiatric institution. Your Position/Relationship with the Patient: You are a physician who works at the local psychiatric institution. Jake was sent to you and you would like to provide some treatment for him. Statement: It is appropriate that you gain access to all paper and electronic records of Jake's full medical history at the hospital.

C5: It is appropriate that the hospital privacy policy gives emergency shelters or support groups full access to a patient's medical record if the patient is an adult and is found to be a victim of serious physical abuse.
E5: Patient Condition: Allison Weill was found to be a victim of serious physical abuse and was sent to the local emergency shelter. Your Position/Relationship with the Patient: You are a physician who works for the emergency shelter for women and children in the local community. Allison was sent to you and you would like to offer some help and provide some resources for her. Statement: It is appropriate that

you gain access to all paper and electronic records of Allison's full medical history at the hospital.

C7: It is appropriate that the hospital privacy policy gives a consulting physician full access to a patient's medical record when he has taken part in the patient's care.
E7: Patient Condition: Alex Miller is a patient that came to the hospital yesterday for diarrhea. Your Position/Relationship with the Patient: You completed your residency in Gastroenterology and have been practicing medicine for a few years. You are the consulting physician for Alex. You have closely examined his condition. Now you are about to make a professional diagnosis and prognosis regarding Alex's disease and offer a treatment plan to the attending physician and nurse practitioner. Statement: It is appropriate that you gain access to all paper and electronic records of Alex's full medical history.

C9: It is appropriate that the hospital privacy policy gives a specialty physician full access to a patient's medical record when he is temporarily responsible for the patient and carrying out a specialty treatment.
E9: Patient Condition: Adam Turner came into the hospital yesterday. After he was diagnosed with bronchitis, he was transferred for specialty treatment. Your Position/Relationship with the Patient: You have completed your residency in Pulmonary Medicine, and have been practicing medicine for a few years. You will be providing specialty treatment for Adam. Statement: It is appropriate that you gain access to all paper and electronic records of Adam's full medical history.

In this second group of questions, the subject decisions differed significantly ($p < 0.05$), with the experimental group making tighter decisions:

C6: It is appropriate that the hospital privacy policy gives a clerical worker full access to a patient's medical record if he needs the patients information for administrative purposes.
E6: Patient Condition: Nina Martin is a patient who came to the Hospital for food poisoning. Your Position/Relationship with the Patient: You are a clerical worker who works at the hospital. It would be beneficial for you to gain access to Nina's medical history for administrative purposes. Statement: It is appropriate that you gain access to all paper and electronic records of Nina's full medical history.

C8: It is appropriate that the hospital privacy policy gives a government official full access to a patient's medical record if he needs the patients information to carry out a public health operation.
E8: Patient Condition: Kristen Rogers is a patient who came in to the hospital for a heart attack. Your Position/Relationship with the Patient: You are a government official who works for the Department of Public Health. To improve public health conditions and reduce healthcare costs, you took on the task of performing a quality assessment on the quality of care offered by hospitals. You are directed to Kristen's information by her primary physician. Statement: It is appropriate that you gain access to all of Kristen's paper and electronic records of her full medical history.

In the third group of questions, the subject decisions did not differ significantly ($p \geq 0.05$):

C10: It is appropriate that the hospital privacy policy gives a senior medical professor full access to a patient's sensitive medical records such as the psychiatric record if the professor is giving clinical education on this topic and needs the patients information as part of his lecture.
E10: Patient Condition: Paul Smith was diagnosed with anxiety disorders at the hospital. Your Position/Relationship with the Patient: You are a senior medical professor, and you will be giving a clinical lesson on anxiety disorders. You are directed to Paul's information by his primary physician. Paul displays many symptoms that closely match the content of your lesson. Statement: It is appropriate that you keep Paul anonymous and display all paper and electronic records of his psychiatric history in your presentation.

C11: It is appropriate that the hospital privacy

policy gives a Registered Nurse Practitioner full access to a patient's medical record when he has taken part in the patient's care.
E11: Patient Condition: Darrick Johnson was sent to the hospital for peripheral arterial disease. Your Position/Relationship with the Patient: You are a registered nurse practitioner and have worked in the hospital for over five years. You are the primary nurse responsible for Darrick's care during his stay. Statement: It is appropriate that you gain access to all paper and electronic records of Darrick's full medical history.

C12: It is appropriate that the hospital privacy policy gives a resident full access to a patient's medical record when he has taken part in the patient's care.
E12: Patient Condition: Andy Jacobs is a patient that came into the hospital for recurring hives. Your Position/Relationship with the Patient: As a second-year resident specialized in Dermatology, you are now in charge of Andy's care along with a physician assistant and a couple of medical students, but you are not Andy's attending doctor. Statement: It is appropriate that you gain access to all paper and electronic records of Andy's full medical history.

C13: It is appropriate that the hospital privacy policy gives a physician full access to a patient's medical record from another hospital when he is providing treatment to the patient during an emergency.
E13: Patient Condition: Melissa Gardner was just in a traffic accident and was sent to the hospital. Your Position/Relationship with the Patient: You have completed your residency in Cardiology and have been practicing medicine for a few years. As the physician on-call tonight, you will be providing emergency treatment to Melissa. Statement: It is appropriate that you gain access to all paper and electronic records of Melissa's full medical history kept at another hospital.

References

[1] L. Van Boven, D. Dunning, and G. Loewenstein. Egocentric Empathy Gaps Between Owners and Buyers: Misperceptions of the Endowment Effect. *Journal of Personality and Social Psychology*, 79:66–76, 2000.

[2] M. Donner, D. Nochin, D. Shasha, and W. Walasek. Algorithms and Experience in Increasing the Intelligibility and Hygiene of Access Control in Large Organizations. In *Proceedings of the IFIP TC11/WG11.3 Fourteenth Annual Working Conference on Database Security*. Kluwer, 2001.

[3] E. W. Dunn and S. A. Laham. Affective Forecasting: A User's Guide to Emotional Time Travel. In J. Forgas, editor, *Affect in Social Thinking and Behavior*. Psychology Press, 2006.

[4] A. Ferreira, R. Cruz-Correia, L. Antunes, and D. Chadwick. Access Control: How Can it Improve Patients' Healthcare? *Studies In Health Technology And Informatics*, 127:65–76, 2007.

[5] P. Garrett and J. Seidman. EMR vs EHR—What is the Difference? *HealthITBuzz*, January 2011.

[6] C. Gunter, D. Liebovitz, and B. Malin. Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems. *IEEE Security and Privacy*, 9(5):48–55, 2011.

[7] L. Gurley and B. Rose. Advantages and Disadvantages of the Electronic Medical Record. In *American Academy of Medical Administrators*, 2004.

[8] R. Koppel, T.B. Wetterneck, J.L. Telles, and B. Karsh. Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety. *Journal of the American Medical Informatics Association*, 15:408–423, 2008.

[9] D. Povey. Optimistic Security: A New Access Control Paradigm. In *Proceedings of the 1999 New Security Paradigms Workshop*, pages 40–45, 2000.

[10] E. Pronin, C. Olivola, and K. Kennedy. Doing Unto Future Selves As You Would Do Unto Others: Psychological Distance and Decision Making. *Personality and Social Psychology Bulletin*, 34:224–237, 2007.

[11] J. Saleem, A. Russ, A. Neddo, P. Blades, B. Doebbeling, and B. Foresman. Paper Persistence, Workarounds, and Communication Breakdowns in Computerized Consultation Management. *International Journal of Medical Informatics*, 80(7):466–479, 2011.

[12] R. Sandhu, D. Ferrailo, and R. Kuhn. The NIST Model for Role-Based Access Control: Towards a Unified Standard. In *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, 2000.

[13] S. Sinclair and S.W. Smith. Preventative Directions For Insider Threat Mitigation Via Access Control. In S. Stolfo et al., editors, *Insider Attack and Cyber Security: Beyond the Hacker*, pages 173–202. Springer-Verlag Advances in Information Security 39, 2008.

[14] S. Sinclair and S.W. Smith. What's Wrong with Access Control in the Real World? *IEEE Security and Privacy*, 8(4):74–77, 2010.

[15] S. Trudeau, S. Sinclair, and S. Smith. The Effects of Introspection on Creating Privacy Policy. In *WPES 09: Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, pages 1–10, 2009.